To AV, or not to AV?

Do you need antivirus (AV) products on smartphones and tablets?

Stuart G

"Do I need to install AV?" is one of the questions many organisations have asked after reading our EUD guidance. The guides provide administrators and risk owners detailed advice for many configuration options, but on the whole we don't spend much time in the guidance specifically discussing the use of antivirus (AV) or anti-malware products.

So in this blog we'll talk about the thought processes behind deciding on using AV on Android and iOS. Windows Desktop and macOS are a bit different, so we'll come back to those in the future.

Finally, we'll mention the most recent changes we've made to the EUD guidance to help better address this question.

How we got here

AV products traditionally worked by scanning every file on a device and looking for malware by spotting known signatures, but advances in malware and changes in underlying platforms have limited the effectiveness of this approach. Whilst malware is more capable, many risks that traditional AV products protected against – and more – are now mitigated by default by the platform at no extra cost. Our *Secure by Default* philosophy is all about promoting this kind of development.

As these features are now commonplace, it's reasonable to ask if you still need to use AV on your mobile devices.

In our EUD guidance, for mobile platforms we recommend that administrators only allow apps to come through the official app stores. This means that all users benefit from the security checks that take place on the applications that are part of those app stores.

Even so, around 0.05% of Android users who get their apps exclusively from the Google Play end up with a Potentially Harmful Application (PHA) on their device at some point, and there have been instances of PHAs in the iOS App Store too. So some administrators and risk owners might want to consider allow listing– also recommended in our guidance – to allow only an approved set of apps from the stores to be installed.

Implementing allow listing means that administrators can check if the app a user has requested balances business need with security risk appropriately, and that the app's developers have a good reputation. Allow listing can be reliably enforced on modern devices because of the use of code signing to identify apps and their developers.

Whether allow listing is implemented or not, if a PHA somehow gets into an official app store and is later found to be malicious, the app store itself can both remove the app from their stores, but also delete the PHA from your users' devices in exactly the same way AV can.

When wouldn't you need AV?

What this means then, is that if you have followed our EUD guidance and are deploying up-to-date devices with allow listing and sandboxing, and you're getting your apps through the official app stores, you're not really mitigating any additional risks by using third-party antivirus or anti-malware products. This view is shared by Google's head of product security who reckons that 99% of Android users do not need any additional security software on their devices.

Even if your users are in that group that isn't covered by allow listing, and they can download or install apps outside of the official app store channels, on Android, there's also Verify Apps which acts much like a traditional AV product and regularly scans apps, reducing the risk of malicious apps being loaded onto the platform from an untrusted source.

On iOS, the only real way to sideload apps is having jailbroken it, which we've blogged about preventing previously.

When might you need AV?

You may want to consider using AV on older devices that are not able to be updated to include the latest security features such as Verify Apps, though we'd always advise using up-to-date and supported devices at all times to really minimise the risk from infection.

Some AV products have other security functionality which you might want for your platform - essentially using the AV as an endpoint security product. For example, AVs may be able to lock down individual photos, sensitive documents, or apps with PINs; other features may include taking pictures of the user when they try and fail to unlock the device – something similar to a camera trap. However, do consider the source and reputation of your AV product as issues have been found with them in the past. Do some research and also check their impact on the device battery life and performance.

Being clearer in our guidance

As a result of the conversations we've been having on this topic, we've taken the opportunity to update our Android and iOS EUD guidance to include some of these details.

If you have any further thoughts or questions on the topic then pop them below!

Stuart G
EUD Security Research

WRITTEN BY

Stuart G

PUBLISHED

7 June 2017

WRITTEN FOR

Large organisations

Public sector

Cyber security professionals

PART OF BLOG

NCSC publications